AMENDMENTS TO CLAIMS

Please amend claims 1-5, 7 and 11-13, as shown in marked form below.

1. (Currently Amended) A method to prevent fraudulent use of a wireless unit that is roaming in a visited system, the method comprising:

~~A.~~ as a part of registration of the wireless unit with a visited mobile switching center (MSC-V) of the visited system, causing the MSC-V to implement denial of originating communication service with respect to the wireless unit;

~~B.~~ after the registration of the wireless unit with the MSC-V and the denial of the originating communication service with respect to the wireless unit, receiving at the MSC-V a code and identification information from the wireless unit;

~~C.~~ in response to the receipt of the code, causing the MSC-V to transmit a message including the identification information to a verification element functionally connected to the visited system and a home system of the wireless unit;

~~D.~~ in response to receipt of the message, causing the verification element to carry out a verification of the identification information;

~~E.~~ in response to making a positive verification, causing the verification element to transmit a response to the MSC-V, the response including the positive verification; and

~~F.~~ based on the positive verification received in the response, causing the MSC-V to remove the denial of the originating communication service with respect to the wireless unit, thereby initiating the communication service with respect to the wireless unit

~~whereby fraudulent use of the wireless unit is prevented by the denial of the originating communication service with respect to the wireless unit even though the wireless unit is registered until the wireless unit provides the identification information that is positively verified.~~

2. (Currently Amended) The method of Claim 1, wherein ~~in action E~~ the response including the positive verification comprises origination/termination service information; and

wherein the method further ~~comprising~~ comprises:

~~G.~~ causing the MSC-V to update information the MSC-V retains in a visitor location resister (VLR) relating to the wireless unit with the origination/termination service information; and

~~H.~~ after removal of the denial of the originating communication service with respect to the wireless unit, causing the MSC-V to provide communication services to the wireless unit based on the origination/termination service information.

BT
C1
cont'd

3. (Currently Amended) The method of Claim 1, wherein ~~in action G~~ the message including the identification information comprises a feature request message, and wherein the identification information comprises a personal identification number (PIN), ~~and wherein the verification element comprises an international gateway~~; and

wherein ~~action C~~ causing the MSC-V to transmit a message comprises causing the MSC-V to transmit the feature request message including the PIN to the ~~international~~ gateway verification element.

4. (Currently Amended) The method of Claim 3, wherein the response comprises a feature request response; and

wherein ~~action E~~ causing the verification element to transmit a response to the MSC-V comprises causing the ~~international gateway~~ verification element to transmit a feature request response to the MSC-V.

5. (Currently Amended) The method of Claim 1, wherein prior to ~~action B of~~ receiving at the MSC-V the code and the identification information from the wireless unit, the method ~~The present invention includes methods, systems, and apparatus that substantially prevent the fraudulent use of wireless units roaming in visited systems.~~

~~Generally stated, a visited mobile switching center (MSC-V) carries out a registration of a wireless unit that is roaming in the visited system. After successful~~

registration, the MSC-V implements at least the denial of originating communication service to the wireless unit. In other words, the wireless unit is allowed to receive calls, but is not allowed to make calls. Advantageously, the present inventions substantially prevent the fraudulent use of wireless units roaming in visited systems by requiring such units to undergo a verification or authentication process prior to being allowed to make calls.

In particular, as a first action in the authentication process of a wireless unit roaming in a visited system, the wireless unit provides a code and identification information in a call. The MSC-V recognizes the code as a feature request (or the like) with respect to a network element. The MSC-V routes the feature request including the identification information to the network element. In response to receipt of the identification information, the network element checks whether the wireless unit is a verified or authentic unit. If the wireless unit is a verified unit, then the network element responds to the MSC-V with a verification in a feature request response. Based on the verification, the MSC-V removes the denial of originating communication service with respect to the wireless unit. In other words, based on the verification, the MSC-V allows the wireless unit to initiate a call.

In sum, the inventors have determined that fraudulent use of wireless units roaming in a visited system occurs most often with respect to wireless units that are used to fraudulently to make (rather than to receive) calls. Thus, the present inventions implement an authentication or verification process that must be successfully negotiated prior to a wireless unit roaming in a visited system being allowed to make a call.

Objects

comprises:

receiving at the MSC-V a call attempt from the wireless unit; and

causing the MSC-V in response to the call attempt to provide the wireless unit with an announcement.

6. (Original) The method of Claim 5, wherein the announcement comprises an instruction to the wireless unit to dial the code and provide the identification information.

7. (Currently Amended) A system to prevent fraudulent use of a wireless unit that is roaming in a visited system, the system comprising:

a visited mobile switching center (MSC-V) operative

to carry out a registration of the wireless unit in the visited system,

to implement, after the registration, denial of originating communication service with respect to the wireless unit,

to receive, after the denial, a code and identification information in a call from the wireless unit;

to recognize the code as a feature request with respect to a network element, and

to route a feature request message including the identification information to the network element;

the network element operative in response to receipt of the identification information to provide a verification in a feature request response to the MSC-V, the network element being functionally connected to the visited system and a home system of the wireless unit; and

the MSC-V also operative to remove the denial if the verification comprises a positive verification.

8. (Original) The system of Claim 7 wherein the feature request response from the network element comprises origination/termination service information with respect to the wireless unit;

wherein the MSC-V comprises a visitor location register (VLR) including information relating to the wireless unit; and

wherein the MSC-V is operative to update the information in the VLR with the origination/termination service information.

9. (Original) The system of Claim 8, wherein, after the removal of the denial, the MSC-V is operative to provide communication services to the wireless unit based on the origination/termination service information.

10. (Original) The system of Claim 7, wherein, after the registration of the wireless unit with the visited system and prior to the denial of originating communication service to the wireless unit, the MSC-V is operative to receive a call attempt from the wireless unit, and in response to the call attempt, is operative to provide an instruction to the wireless unit to dial the code and provide the identification information.

11. (Currently Amended) A method to prevent fraudulent use of a wireless unit roaming in a visited system, comprising:

locking the wireless unit prior to a registration of the wireless unit;

performing a first authentication process to unlock the wireless unit;

~~A.~~ in response to unlock of the wireless unit, carrying out ~~a~~the registration of the wireless unit in the visited system including validation of the wireless unit with a home system of the wireless unit; and

~~B. implementing~~ performing, in response to the registration, a second authentication process implementing a denial of originating communication service to the wireless unit.

12. (Currently Amended) The method of Claim 11, further comprising:

~~C.~~ in response to a positive verification of identification information received from the wireless unit during the second authentication process, providing the originating communication service to the wireless unit.

13. (Currently Amended) The method of Claim 11, further comprising:

~~C.~~ receiving a call attempt from the wireless unit; and

D. in response to the call attempt, providing an announcement to the wireless unit.

14. (Original) The method of Claim 13, wherein the announcement comprises an instruction to the wireless unit to dial a code and provide identification information.

15. (New) The method of Claim 11, wherein performing a first authentication process comprises entering a personal identification number to unlock the wireless unit.

16. (New) The method of Claim 11, wherein performing a second authentication process comprises performing the second authentication process during a predetermined time or during a plurality of predetermined times.